Helmut Krcmar · Claudia Eckert
Alexander Roßnagel · Ali Sunyaev
Manuel Wiesche *Hrsg.*

RESEARCH

Management sicherer Cloud-Services

Entwicklung und Evaluation dynamischer Zertifikate

Springer Gabler

Management sicherer Cloud-Services

Helmut Krcmar · Claudia Eckert
Alexander Roßnagel · Ali Sunyaev
Manuel Wiesche
(Hrsg.)

Management sicherer Cloud-Services

Entwicklung und Evaluation dynamischer Zertifikate

Springer Gabler

Herausgeber
Helmut Krcmar
München, Deutschland

Claudia Eckert
München, Deutschland

Alexander Roßnagel
Kassel, Deutschland

Ali Sunyaev
Kassel, Deutschland

Manuel Wiesche
München, Deutschland

ISBN 978-3-658-19578-6 ISBN 978-3-658-19579-3 (eBook)
https://doi.org/10.1007/978-3-658-19579-3

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Gabler ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Für viele Unternehmen ist die Nutzung von Cloud-Diensten ein wesentlicher Bestandteil zur Digitalisierung ihrer Unternehmensabläufe, die Vorteile im Bereich der Kosten, der Unternehmenssteuerung und in der Wettbewerbsfähigkeit bietet. Allerdings schrecken Unternehmen vor der Investition in Cloud Computing zurück, weil die Einhaltung von Datenschutz und Datensicherheit ungewiss ist. Auch bestehende Zertifikate zum Nachweis der Einhaltung von Datenschutz- und Datensicherheitskriterien sind nicht ausreichend, da sie aufgrund der hohen Dynamik der Cloud-Technologien zu unflexibel sind.

Die Herausforderung der Dynamik des Markts kann durch die zurückblickende Perspektive bestehender Zertifikate nicht gelöst werden. Bestehende Zertifikate beziehen sich immer nur auf einen Zustand, der in der Vergangenheit liegt - haben aber zugleich einen Gültigkeitszeitraum von einem bis drei Jahren. Weiterhin werden Cloud-Services in vielen Fällen als Lieferkette mehrerer Dienstleistungen (Co-Lokation, Managed Service Anbieter, Cloud Anbieter, etc.) erbracht. Die Komplexität der Bündelung mehrerer Dienste erhöht die Wahrscheinlichkeit technischer, organisatorischer oder rechtlicher Änderungen, die Auswirkungen auf die jeweiligen Zertifikatsaussagen haben können. Zudem sind für den Anwender die Zertifikate mit unterschiedlichen Schwerpunkten und Ausrichtungen oft nicht transparent und kaum vergleichbar.

Um diesen aktuellen Herausforderungen von Cloud-Service-Zertifikaten zu begegnen, ist es erforderlich, dass Datenschutz- und Datensicherheitsanforderungen (teil-) automatisiert und kontinuierlich überprüft sowie anschließend zertifiziert werden. Hier setzt das Projekt „Next Generation Certification“ (NGCert), gefördert durch das Bundesministerium für Bildung und Forschung (BMBF), an. Das Projekt hat das Ziel, eine genauere Aussage über die Einhaltung der verschiedenen Anforderungen mittels dynamischer Verfahren zu erzielen. Mittels dieser dynamischen Verfahren werden kontinuierlich und (teil)automatisiert kritische Anforderungen eines Zertifikats überprüft und das Ergebnis der Überprüfung stets aktuell dargestellt. Eine solche dynamische Zertifizierung bietet einen kontinuierlichen Nachweis über die Güte und Qualität der vom Zertifikat verlangten Kontrollen beim Cloud-Service-Provider. Die dynamische Zertifizierung ermöglicht somit die Übertragung des vertrauensbildenden Prozesses der Zertifizierung in die dynamische und sich schnell verändernde Welt der Cloud-Services. Sie liefert eine rechtsverbindliche Grundlage in der Entscheidungsfindung zur Auswahl von Cloud-Services.

Im Rahmen des Projekts NGCert wurde ein dynamisches Zertifizierungsumfeld erarbeitet und pilotiert, das alle Perspektiven auf Cloud-Zertifikate berücksichtigt und somit sowohl Cloud-Kunden, Cloud-Service-Provider und Cloud-Zertifizierer unterstützt:

Erstens benötigen Cloud-Kunden für ihre Entscheidung strukturierte und verlässliche Information über einen Cloud-Service. Dazu werden Cloud-Services systematisiert und Entschei-

dungskriterien diskutiert. Zudem will NGCert insbesondere kleine und mittelständische Unternehmen unterstützen, indem die entwickelten Zertifizierungsdienste deren spezifische Anforderungen adressieren. Zweitens entwickelt das Projekt dynamische Metriken, mit denen sich Cloud-Services leichter vergleichen und die Servicequalitäten bestimmen lassen. Hierdurch können rechtlich belastbare Aussagen zu service- und datenschutzbezogenen Eigenschaften getroffen werden. Drittens entwickelt das Projekt vertrauensunterstützende Zertifizierungsdienste für mehr Transparenz in der Beschaffung, Auswahl und Einsatz von Cloud-Services.

Mit der so geschaffenen Transparenz und Vergleichbarkeit wird es im Gegenzug für die Cloud-Service-Anbieter noch wichtiger, marktgerechte Angebote zu schaffen, die den Anforderungen der Kunden an Qualität, Vertrauenswürdigkeit und Verlässlichkeit genügen. NGCert hilft Cloud-Service-Anbieter hierbei, nachweislich die Service-Bereitstellung zu kommunizieren und durch unabhängige Dritte zu verifizieren.

Ebenso profitieren Cloud-Zertifizierer von NGCert, indem interaktive Aufgaben (teil-) automatisiert werden und damit das Auditierungsrisiko stark verringert wird. Der hierdurch reduzierte Auditierungsaufwand ermöglicht es den Auditoren, neue und innovative Überwachungsaufgaben zu übernehmen.

Ausgewählte Ergebnisse des Projekts stehen auf der Webseite des Projektes (www.ngcert.de) zum Download bereit. Außerdem wurden die Ergebnisse in Fachverbänden weitergegeben und im Rahmen von Workshops diskutiert. In den entsprechenden wissenschaftlichen Disziplinen wurden die Ergebnisse in Fachzeitschriften veröffentlicht und auf Konferenzen vorgestellt und diskutiert.

Unser Dank gilt dem BMBF und seinem Projektträger VDI/VDE für die Betreuung des Vorhabens. Unser persönlicher Dank gebührt Herrn Dr. Ulf Lange (BMBF) und Herrn Dr. Kristian Döbrich (VDI/VDE) für die Unterstützung und Begleitung des Projekts sowie allen beteiligen Projektpartnern und Mitarbeitern für den unermüdlichen und engagierten Einsatz, ohne den dieses Vorhaben nicht möglich gewesen wäre. Dies sind insbesondere Christian Banse, Prof. Dr. Hermann de Meer, Bernhard Doll, Dirk Emmerich, Pascal Grochol, Mario Hoffmann, Johanna Hofmann, Ramona Kühn, Britta Laatzen, Michael Lang, Sebastian Lins, Joachim Lohmann, Christine Neubauer, Georg Pribyl, Philipp Stephanow, Heiner Teigeler und Andreas Weiss.

Danken möchten wir auch unseren Unterstützern außerhalb des geförderten Projektkonsortiums, die mit ihrem Engagement und Expertenrat maßgeblich zum Erfolg des Vorhabens beigetragen haben. Dies sind insbesondere Monika Graß (Grass Consulting), Malte Jäger (Brand's Mill Consultants), Andreas Dangl (Fabasoft), Winfried Heinrich (digital intelligence institute), Dr. Andreas Nutz (FIDES IT Consultants), Oliver Dehning (Hornetsecurity) sowie einige weitere.

Wir hoffen, dem Leser eine spannende und Nutzen stiftende Lektüre an die Hand geben zu können und wünschen dem Abschlussbericht die ihm gebührende weite Verbreitung.

Helmut Krcmar
Claudia Eckert
Alexander Roßnagel
Ali Sunyaev
Manuel Wiesche

Inhaltsüberblick

Abkürzungsverzeichnis

a.A.	Andere Auffassung
a.F.	alte Fassung
ABl.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AkkStelleG	Akkreditierungsstellengesetz
Alt.	Alternative
Art.	Artikel
Aufl.	Auflage
BDSG	Bundesdatenschutzgesetz
Beschl. v.	Beschluss vom
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMBF	Bundesministerium für Bildung und Forschung
BMWi	Bundesministerium für Wirtschaft und Energie
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
CR	Computer und Recht (Zeitschrift)
ders./dies.	Derselbe/dieselbe
DIN	Deutsches Institut für Normung
DSGVO	Datenschutz-Grundverordnung (EU) 2016/679
DSGVO-E	Entwurf für eine Datenschutz-Grundverordnung
DS-RL	Datenschutzrichtlinie (95/46/EG)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt (Zeitschrift)
Eg.	Erwägungsgrund
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten
et al.	et alii (und andere)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union i.d.F. des Vertrags von Lissabon
EWR	Europäischer Wirtschaftsraum
f.	folgende/-r/-s
ff.	fortfolgende/ -r/-s
Fn.	Fußnote(n)
gem.	gemäß
GG	Grundgesetz
GRCh	Charta der Grundrechte der Europäischen Union

HDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
Hrsg.	Herausgeber/in
Hs.	Halbsatz
i.d.F.	In der Fassung
i.d.R.	in der Regel
i.E.	im Ergebnis
i.S.d.	im Sinne des / der
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
IaaS	Infrastructure as a Service
IP	Internetprotokoll
ISO	International Organization for Standardization
IT	Informationstechnik
K&R	Kommunikation & Recht (Zeitschrift)
Kap.	Kapitel
KMU	Kleine und mittlere Unternehmen
KOM	EU-Kommission
LDSG	Landesdatenschutzgesetz
LG	Landgericht
lit.	Litera (Bustabe)
m. Anm.	mit Anmerkung
MMR	Multi-Media-Recht (Zeitschrift)
m.w.N.	mit weiteren Nachweisen
n.F.	neue Fassung
NIST	National Institute of Standards and Technology
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
o.g.	oben genannte/-r/-s
OLG	Oberlandesgericht
PaaS	Platform as a Service
RDV	Recht der Datenverarbeitung (Zeitschrift)
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
Rz.	Randziffer
SaaS	Software as a Service
sog.	sogenannte/-r/-s
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.a.	unter anderem / und andere
u.U.	unter Umständen
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Urt. v.	Urteil vom
UWG	Gesetz gegen den unlauteren Wettbewerb
vgl.	vergleiche
VO	Verordnung
VuR	Verbraucher und Recht – Zeitschrift für Wirtschafts- und Verbraucherrecht
WP	Working Paper

z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZUM	Zeitschrift für Urheber- und Medienrecht

Teil A: Einleitung

1 Motivation, Bausteine und Vorgehensweise

C. Banse, P. Stephanow

1.1 Motivation

Cloud-Services versprechen Unternehmen zahlreiche Möglichkeiten der Kostenersparnis durch Auslagerung von Prozessen und Dienstleistungen in die Cloud. Gerade mittelständische Unternehmen könnten enorm von den Vorteilen von Cloud-Services profitieren. Laut der Studie „Cloud Monitor 2017“[1] von KPMG und bitkom research nutzen bereits 65 % der Unternehmen in Deutschland Cloud-Services. Weitere 18 % planen oder diskutieren den Einsatz. Das Thema Sicherheit und Compliance ist dabei ein wichtiger Faktor. 67 % der Unternehmen sehen, dass der Einsatz von Cloud-Services die Compliance gefährdet. Dies spiegelt sich vor allem dadurch wider, dass über 75 % der Cloud-Service-Kunden erwarten, dass der Provider seinen Hauptsitz im Rechtsgebiet der EU hat. Wenig nachgefragt sind allerdings bisher Angebote im Bereich Public Cloud, mit nur 29 % der Unternehmen. Diese recht niedrige Quote kommt primär durch das immer noch etwas zurückhaltende Verhalten von kleinen und mittelständischen Unternehmen zu Stande. Als größte Hemmnisse gegenüber der Nutzung von Public Clouds stehen laut Studie weiterhin die Befürchtung des unberechtigten Zugriffes auf Unternehmensdaten (52 %) sowie rechtliche und regulatorische Bestimmungen (50 %).

Dies zeigt umso mehr den Bedarf an Implementierung nachweislich vertrauenswürdiger Cloud-Services. Entscheidend ist die Schaffung von Transparenz für die Einhaltung zentraler Sicherheitskriterien. Darüber hinaus ist das System der bestehenden Zertifikate oft nicht ausreichend, weil sie aufgrund der hohen Dynamik der Cloud-Technologien zu unflexibel sind. Der Gültigkeitszeitraum heutiger Zertifikate liegt typischerweise im Bereich von einem bis drei Jahren. Und genau darin besteht das Problem: Cloud-Dienste können sich über die Zeit hinweg verändern, z.B. im Zuge des Austausches zentraler Hardwarekomponenten oder Softwaremodule, Konfigurationsänderungen, oder gar Migration bestimmter Komponenten von einem Rechenzentrum in ein anderes. Die Zertifizierung von Cloud-Services erfordert daher eine neue Herangehensweise, die der Dynamik dieser Dienste gewachsen ist.

Bereits seit einigen Jahren befassen sich daher Forschungsaktivitäten auf nationaler und europäischer Ebene mit der Thematik der sogenannten *dynamischen Zertifizierung*. Deren Ziel liegt darin, bisherige Verfahren durch die Einführung von (teil)-automatisierten Prozessen zu unterstützen, um eine kontinuierliche Überprüfung wichtiger Zertifizierungsanforderungen zu ermöglichen. Daher hat sich das durch das Bundesministerium für Bildung und Forschung

[1] https://home.kpmg.com/de/de/home/themen/2017/03/cloud-monitor-2017.html

H. Krcmar et al. (Hrsg.), *Management sicherer Cloud-Services*,
https://doi.org/10.1007/978-3-658-19579-3_1

(BMBF) geförderte Projekt *„NGCert – Next Generation Certification“*[2] zum Ziel gesetzt, Methoden zum kontinuierlichen Nachweis eines Zertifizierungsstatus zu erforschen und zu entwickeln. Das von Oktober 2014 bis Dezember 2017 laufende Projekt war Teil des Themenfeldes „Sicheres Cloud Computing“ im Rahmen der Hightech-Strategie der Bundesregierung. Im Rahmen des Projektes NGCert wurde untersucht, welche technische, organisatorische und rechtliche Rahmenbedingungen und Anforderungen zum Betrieb eines dynamischen Zertifizierungsdienstes eingehalten werden müssen. So wurden technische Methoden entwickelt, um Zertifizierungskriterien, z.B. an die Verfügbarkeit oder die geographische Lokation eines Cloud-Dienst kontinuierlich abzuprüfen. Inhalt dieses Abschlussbandes ist die Vorstellung der Forschungsergebnisse des NGCert-Projektes.

1.2 Bausteine des NGCert-Projektes

Zur Organisation des Projektes wurde eine Baustein-ähnliche Struktur zugrunde gelegt (siehe Abbildung 1). Die Grundbausteine, *Spezifikation der Anforderungen*, *Design*, *Prototypische Implementierung* sowie die *Validierung durch Feldpartner* bilden die Grundpfeiler des NGCert-Projektes. Begleitend werden diese durch Aktivitäten der *betriebswirtschaftlichen und organisatorischen Betrachtung* sowie der *rechtsicheren Umsetzung*. Besonders das Einbeziehen von rechtlichen Anforderungen bereits während der Entwicklung durch die Methode zur „Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen“ (KORA) stellt hierbei einen deutlichen Mehrwert für alle Beteiligten des Zertifizierungs-Ökosystems dar. Die Betrachtungen aus betriebswirtschaftlicher und organisatorischer Sicht stellen sicher, dass der wirtschaftliche Nutzen und die Akzeptanz einer dynamischen Zertifizierung gegeben sind.

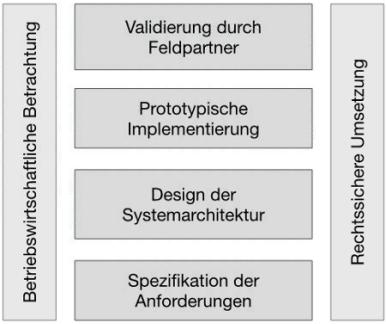

Abbildung 1: Bausteine des NGCert-Projektes

[2] https://www.ngcert.de

Zur operativen Durchführung des Projektes wurde eine iterative Herangehensweise gewählt (siehe Abbildung 2). Die Entwicklung des prototypischen Zertifizierungsdienstes erfolgte anhand von drei vorgesehenen Iterationsstufen:

- Die *Basisbausteine* beinhalten die grundlegenden technischen Komponenten zur Umsetzung einer dynamischen Zertifizierung.
- Der *Basisdienst* erweitert und integriert die Basisbausteine in einen prototypischen Dienst.
- Der *Erweiterte Dienst* ergänzt den Basisdienst um die in der Validation durch externe Partner gewonnen Ergebnisse.

Zum Beginn jeder Projektiteration wurden zunächst Anforderungen aus rechtlichen und technischen Rahmenbedingungen abgeleitet. Diese wurden durch die Definition eines Kennzahlensystems basierend auf Metriken sowie einer Taxonomie zur Beschreibung von Cloud-Services ergänzt. Diese Anforderungen wurden im Laufe der Iterationen in Use-Case-Beschreibungen konsolidiert und bilden die Grundlage für das Design und anschließender prototypischen Implementierung eines dynamischen Zertifizierungsdienstes. Das Ende jeder Iterationsstufe bildet schließlich die Validierung der erarbeiteten Ergebnisse. Je nach Iteration geschah dies in Form von Workshops mit externen Personen oder durch den testweisen Einsatz des Prototyps in Cloud-Umgebungen externer Partner. Begleitet wurden alle Iterationen von einer Betrachtung der rechtsicheren Umsetzung, der organisatorischen und betrieblichen Aspekte, sowie der Akzeptanz von dynamischen Zertifizierungen.

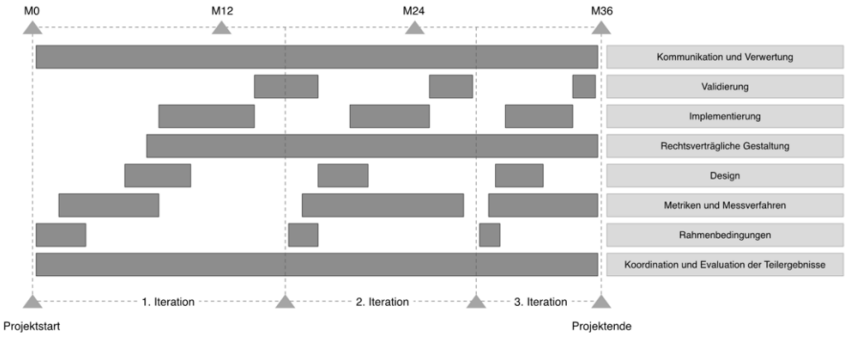

Abbildung 2: Arbeitspakete und Iterationsstufen

1.2.1 Projektpartner

Das vom Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC geleitete Konsortium bestand aus mehreren Partnern aus Wissenschaft, Forschung und Wirtschaft. Die wissenschaftlichen Partner erforschten und entwickelten die grundlegenden Ansätze und Ver-

fahren für das Projekt, während die Unternehmenspartner wirtschaftliche und praktische Anforderungen beisteuerten. So entstand federführend durch die Technische Universität München (TUM), Prof. Krcmar, ein Referenzmodell für die dynamische Zertifizierung. Des Weiteren betrachtete die TUM im Rahmen des Projektes durch empirische Studien die Akzeptanz von dynamischer Zertifizierung. Die Universität Kassel, Prof. Sunyaev, beschäftigte sich mit der konzeptionellen Architektur eines Zertifizierungsdienstes sowie dem Marktpotenzial von dynamischen Zertifizierungen. Gemeinsam mit der TU München wurde ein Wertschöpfungsnetzwerk eines Zertifizierungsökosystems entwickelt.

Das Design und die Umsetzung eines technischen Rahmenwerks für eine dynamische Zertifizierung wurden von Fraunhofer AISEC, Prof. Eckert, übernommen. So wurden unter anderem technische Methoden für die Überprüfung der Verfügbarkeit, Geo-Lokation sowie Sicherheit der Verbindungsverschlüsselung entwickelt. Anknüpfend an das von Fraunhofer AISEC entwickelte Rahmenwerk wurden an der Universität Passau, Prof. de Meer, Messmethoden für das Access Management entwickelt. Die Projektgruppe für verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel, Prof. Roßnagel, übernahm im Rahmen des Projektes die Betrachtung aus rechtlicher Sicht. Insbesondere flossen so bereits während der Entwicklungsphase rechtliche Anforderungen an einen Zertifizierungsdienst ein. Basierend auf den Anforderungen wurden konkrete Handlungsempfehlungen zur Umsetzung eines dynamischen Zertifizierungsdienstes aufgestellt.

Zusammen mit dem Industriepartner EuroCloud entstand ein Vergleich existierender Zertifizierungsstandards zum Nachweis vertrauenswürdiger Cloud Services. Darüber hinaus übernahm EuroCloud Deutschland_eco e.V. als Branchenvertreter die Übertragung der Forschungsergebnisse in die Industrie und Wirtschaft, z.B. durch Workshops und Veranstaltungen sowie das Rückspielen von Anforderungen aus der Industrie in das NGCert-Projekt. Fujitsu als Cloud-Anbieter steuerte wirtschaftliche und praktische Anforderungen bei. Des Weiteren beschäftigte sich Fujitsu mit der Etablierung eines Sicherheitskonzepts zum Einsatz der prototypischen Implementierung.

1.3 Aufbau des Abschlussbandes

Die Inhalte dieses Abschlussbandes gliedern sich in sieben Teile:

- *Auswahl von Cloud Services:* Der erste Themenbereich beschreibt die grundsätzliche Klassifikation von Cloud-Services, z.B. anhand des Dienste-Modells (IaaS, PaaS und SaaS) sowie Kriterien für Unternehmen, anhand derer Cloud-Dienste ausgewählt werden. Zuletzt beschäftigt sich der Themenbereich mit der rechtsverträglichen Gestaltung von Diensten.
- *Vertrauenswürdige Cloud Services:* Im darauf aufbauenden Themenkomplex werden grundsätzliche Möglichkeiten zum Nachweis von vertrauenswürdigen Cloud-

Services aufgezeigt. Hierbei wird ein starker Fokus auf die Möglichkeit der Zertifizierung gelegt und unterschiedliche Zertifikats-Standards werden mit einander verglichen.

- *Dynamische Zertifizierung von Cloud Services:* Aufgrund einer starken Dynamik von Cloud-Services zeigt sich, dass neue Ansätze erforderlich sind, um die Sicherheit und Vertrauenswürdigkeit von Cloud-Services zu gewährleisten. In diesem Themenbereich werden daher Konzepte und Architekturen der dynamischen Zertifizierung, sowohl aus technischer, betriebswirtschaftlicher als auch rechtlicher Betrachtungsweise aufgezeigt.
- *Ein Prototyp zum Nachweis von vertrauenswürdigen Cloud Services:* Ausgehend von der konzeptionellen Betrachtung werden konkrete technische Methoden vorgestellt, um den Nachweis einer dynamischen Zertifizierung zu erbringen. Besonderen Fokus erlangen hierbei sogenannte Testbasierte Messmethoden, welche beispielhaft anhand der Prüfkriterien Access Management, Geolokation und Verfügbarkeit aufgezeigt werden. Die Umsetzung dieser Messmethoden erfolgt hierbei stets unter der Prämisse einer rechtsverträglichen Technikgestaltung.
- *Evaluation des Prototyps* sowie *Akzeptanz und Mehrwehrt von Dienstleistungen zum Nachweis vertrauenswürdiger Services:* Hier wird der Rahmen des Projektes NGCert entstandene Prototyp einer technischen Lösung für dynamische Zertifizierung hinsichtlich der Akzeptanz und Relevanz evaluiert. Darüber hinaus wird aufgezeigt, inwieweit das Konstrukt einer dynamischen Zertifizierung vertrauensfördernd hinsichtlich des Einsatzes von Cloud-Services wirken kann.
- *Handlungsempfehlungen:* Der letzte Themenblock befasst sich schließlich mit konkreten Handlungsempfehlungen aus rechtlicher, organisatorischer und technischer Sicht. Die Empfehlungen richten sich an alle Beteiligten eines Zertifizierungs-Ökosystems, vom Cloud-Service-Provider, über den Auditor bis zum Kunden des Cloud-Services.

Während Projekte wie NGCert den Grundstein für eine dynamische Zertifizierung gelegt haben, gilt es noch einige Herausforderungen zu meistern. Eine der zentralen Herausforderung der Zukunft ist das Inkrafttreten der europäischen Datenschutz-Grundverordnung. Durch diese wird stärker nicht nur der Nachweis der Datensicherheit relevant, sondern auch des Datenschutzes im Zusammenhang mit der Verarbeitung personenbezogener Daten. Hier gilt es, neue Standards in der Zertifizierung zu schaffen, sowie konkrete rechtliche Handlungsempfehlungen für Cloud Service-Kunden, -Zertifizierer und -Provider abzuleiten.

Teil B: Auswahl von Cloud-Services

2 Klassifikation von Cloud-Services

S. Lins, A. Sunyaev

In diesem Kapitel werden die Grundlagen zu Cloud Computing kurz erläutert. Cloud Computing bezeichnet ein Modell, welches einen flexiblen und bedarfsorientierten Zugriff auf einen gemeinsam genutzten Pool von konfigurierbaren IT-Ressourcen (darunter Netzwerke, Server, Speicher oder Anwendungen) ermöglicht, die jederzeit und überall über das Internet oder einem Netzwerk abgerufen werden können. Zur Klassifikation von Cloud-Services werden die grundlegenden Charakteristiken des Cloud Computings sowie die Service- und Bereitstellungsmodelle beschrieben.

This chapter introduces the term cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This chapter briefly describes major cloud computing characteristics as well as service and deployment models.

Das Forschungsprojekt NGCert wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) gefördert (Förderkennzeichen: 16KIS0079).

H. Krcmar et al. (Hrsg.), *Management sicherer Cloud-Services*,
https://doi.org/10.1007/978-3-658-19579-3_2

2.1 Cloud Computing

In der Fachliteratur existieren eine Vielzahl von Definitionen und Erklärungsansätzen von Cloud Computing (Leimeister et al. 2010; Marston et al. 2011; Schneider and Sunyaev 2015). Dabei hat sich die Definition des National Institute of Standards and Technology (NIST) in der Fachwelt als Grundlage etabliert. Nach dieser Definition bezeichnet Cloud Computing ein Modell, welches einen flexiblen und bedarfsorientierten Zugriff auf einen gemeinsam genutzten Pool von konfigurierbaren IT-Ressourcen ermöglicht, die jederzeit und überall über das Internet oder einem Netzwerk abgerufen werden können (Mell and Grance 2011). Darunter fällt beispielsweise der Zugriff auf Netzwerke, Server, Speicher oder Anwendungen. Cloud-Services werden mit minimalem Managementaufwand und geringer Interaktion mit dem Cloud-Service-Provider schnell bereitgestellt und können möglichst automatisch an den individuellen Bedarf der Cloud-Service-Kunden angepasst werden. Ferner zeichnet sich Cloud Computing durch fünf spezielle Charakteristiken aus und man unterscheidet drei Service- und vier Bereitstellungsmodelle. Diese werden im Folgenden erläutert.

2.1.1 Charakteristiken des Cloud-Computings

Die für Cloud Computing kennzeichnenden Charakteristiken sind der bedarfsgerechte Zugriff, eine Netzwerkanbindung, die Möglichkeit zur Ressourcenbündelung, eine hohe Skalierbarkeit und eine verbrauchsabhängige Bezahlung (Mell and Grance 2011; Sunyaev and Schneider 2013).

Bedarfsgerechter Zugriff (On-demand Self-service). Der bedarfsgerechte Zugriff ermöglicht es Cloud-Service-Kunden selbstständig und nahezu unmittelbar Leistungsparameter der in Anspruch genommenen Cloud-Services anzupassen. Dies kann insbesondere automatisch und ohne menschliche Interaktion mit den jeweiligen Cloud-Service-Providern durchgeführt werden. So ist es beispielsweise möglich, je nach aktuellem Bedarf, erhaltene Rechen-, Speicher- oder Bandbreitenkapazitäten zu erhöhen oder zu reduzieren.

Netzwerkanbindung (Broad Network Access). Cloud-Services werden über ein Breitbandnetzwerk bereitgestellt, in der Regel über das Internet. Cloud-Services nutzen standardisierte Kommunikationsschnittstellen und können mit einer Vielzahl von Endgeräten benutzt werden, darunter beispielsweise Smartphones, Tablets oder Laptops.

Ressourcenbündelung (Resource Pooling). Die vom Cloud-Service-Provider bereitgestellten Ressourcen werden durch eine Multi-Mandanten-Architektur von mehreren Cloud-Service-Kunden gleichzeitig genutzt. Dabei werden die physischen und virtuellen Ressourcen je nach Bedarf dynamisch den verschiedenen Cloud-Service-Kunden zugeteilt. Cloud-Service-Kunden können hierbei nicht immer den exakten Standort feststellen, an dem sich die genutzten Ressourcen befinden. Jedoch ist eine grobe Eingrenzung hinsichtlich des Landes, der Region oder des Rechenzentrums in einigen Fällen möglich.

Skalierbarkeit (Rapid Elasticity). Bereitgestellte Ressourcen können flexibel und schnell, in einigen Fällen vollautomatisch, erhöht oder freigegeben werden, um so die Ressourcen auf den aktuellen Bedarf abzustimmen. Unter anderem deshalb entsteht für den Cloud-Service-Kunden der Eindruck, dass Ressourcen nahezu unbegrenzt scheinen und zu jeder Zeit in jedem Ausmaß verfügbar sind.

Verbrauchsabhängige Bezahlung (Measured Service). Um Cloud-Services messbar und transparent zu gestalten, kontrollieren und optimieren Cloud-Services den Ressourcenverbrauch anhand von serviceabhängigen Kennzahlen, beispielsweise dem Speicherplatz, der Rechenleistung oder der Bandbreite. Dadurch kann eine bedarfsgerechte Abrechnung angeboten und durchgeführt werden. Zudem wird die Ressourcennutzung überwacht, kontrolliert, protokolliert und kommuniziert, sodass sowohl für den Cloud-Service-Kunden, als auch für den Cloud-Service-Provider, Transparenz über die Nutzung geschaffen wird.

2.1.2 Service-Modelle

Im Cloud Computing kann ferner zwischen den drei grundlegenden Service-Modellen Software as a Service (SaaS), Platform as a Service (PaaS) sowie Infrastructure as a Service (IaaS) unterschieden werden (Schneider and Sunyaev 2015; Mell and Grance 2011). Diese Servicemodelle repräsentieren gemeinsam den technischen Grundansatz von Cloud Computing, in dem Software, Plattform und Infrastruktur als aufeinander aufbauende Schichten verstanden werden. Hierbei ermöglicht und unterstützt die Infrastruktur eine Plattform, während eine Plattform zur Ausführung von Software genutzt wird.

Software as a Service (SaaS). Der Cloud-Service-Kunde kann mittels verschiedener Geräte entweder über ein Thin-Client-Interface, beispielsweise einem Web-Browser, oder über ein entsprechendes Anwendungsinterface auf angebotene Softwareanwendungen zugreifen. Der Cloud-Service-Kunde hat hierbei keine Kontrolle über die zugrundeliegende Cloud-Infrastruktur, sondern kann nur spezifische Anwendungseinstellungen vornehmen.

Platform as a Service (PaaS). Der Cloud-Service-Kunde kann selbstentwickelte oder erworbene Anwendungen auf der Cloud-Infrastruktur des Cloud-Service-Providers installieren und betreiben. Hierzu werden Programmiersprachen, Programmbibliotheken oder weitere vom Cloud-Service-Provider unterstützte Dienste und Werkzeuge genutzt. Ähnlich wie bei dem Software-as-a-Service-Modell hat der Cloud-Service-Kunde keine Kontrolle über die zugrundeliegende Cloud-Infrastruktur. Auf der anderen Seite kann er eigene installierte oder ausgeführte Anwendungen verwalten und kann gegebenenfalls eine limitierte Anzahl von Einstellungen in der entsprechenden technischen Anwendungsumgebung durchführen.

Infrastructure as a Service (IaaS). Der Cloud-Service-Kunde erhält Zugang zu Hardwareressourcen des Cloud-Service-Providers, darunter fallen beispielsweise Rechenleistung, Speicherkapazitäten oder Netzwerke. Diese kann er zur Installation und zum Betrieb beliebiger

Software verwenden, beispielsweise Betriebssysteme oder Anwendungen. Ihm obliegt die Kontrolle über Betriebssysteme, Speicher und installierten Anwendungen, gegebenenfalls auch über ausgewählte Netzwerkressourcen, beispielsweise über Firewalls, jedoch nicht über die zugrundeliegende Cloud-Infrastruktur.

Darüber hinaus finden sich in der Praxis und Literatur eine Vielzahl von weiteren Service-Modellen, beispielsweise Database as a Service oder Security as a Service.

Tabelle 2-1 listet beispielhaft weitere Service-Modelle auf und ordnet sie den grundlegenden Modellen Infrastructure, Platform und Software as a Service zu. Im Folgenden wird nur zwischen diesen drei Modellen unterschieden.

Tabelle 2-1. Weitere Cloud-Service-Modelle und deren Zuordnung zu den grundlegenden Service-Modellen Software, Platform und Infrastructure as a Service.

Service-Modell	Grundlegende Service-Modelle			Beispielhafte Literatur
	SaaS	PaaS	IaaS	
Security as a Service	●	-	-	Sharma et al. (2016)
Search as a Service	●	-	-	Dašić et al. (2016)
Testing as a Service	-	●	-	Linthicum (2009)
Database as a Service	-	●	-	Linthicum (2009)
Network as a Service	-	-	●	Soares et al. (2011)
Rendering as a Service	-	-	●	Annette et al. (2015)

2.1.3 Bereitstellungsmodelle

Zusätzlich zu den oben definierten Service-Modellen wird zwischen den vier grundlegenden Bereitstellungsmodellen (engl.: „Deployment Models“) Private-, Community-, Public- und Hybrid-Cloud unterschieden (Mell and Grance 2011; Schneider and Sunyaev 2015). Darüber hinaus wird das Bereitstellungsmodell Virtual-Private-Cloud oft in der Literatur und Praxis angeführt (Dillon et al. 2010; Amazon Web Services 2015).

Private-Cloud. Die Cloud-Infrastruktur wird nur durch eine einzelne Organisation und deren Mitglieder genutzt. Sie kann sowohl von der Organisation, Dritter oder einer Kombination dieser besessen, verwaltet und betrieben werden. Ferner muss sich die Cloud-Infrastruktur dafür nicht zwingend lokal bei der Organisation befinden.

Public-Cloud. Die Cloud-Infrastruktur kann durch die allgemeine Öffentlichkeit genutzt werden. Unternehmen, akademische oder staatliche Organisationen, oder eine Kombination dieser besitzen, verwalten und betreiben die Cloud-Infrastruktur.

Community-Cloud. Die Cloud-Infrastruktur wird ausschließlich durch eine Gruppe von Organisationen genutzt, welche ähnliche Anforderungen an den Cloud-Service stellen. Eine

oder mehrere Organisationen der Community, Dritte oder eine Kombination dieser Parteien besitzen, verwalten und betreiben die Cloud-Infrastruktur. Auch hierbei muss sich die Cloud-Infrastruktur dafür nicht zwingend lokal bei der Organisation bzw. den Organisationen befinden.

Hybrid-Cloud. Die Cloud-Infrastruktur besteht aus einer Kombination von zwei oder mehreren der oben beschriebenen Modelle. Die einzelnen Infrastrukturen bleiben als Einheit erhalten, werden jedoch durch standardisierte oder proprietäre Technologien verbunden. Dies ermöglicht die Übertragung von Daten und Anwendungen zwischen den angebundenen Infrastrukturen.

Virtual-Private-Cloud. Erstmals wurde der Begriff „Virtual-Private-Cloud" von Amazon Web Services (AWS) eingeführt als deren neues Produkt „Amazon VPC" vorgestellt wurde (Amazon Web Services 2015). Beim Virtual-Private-Cloud-Modell wird die Infrastruktur de facto für eine einzelne Organisation bereitgestellt, die mehrere Nutzer (zum Beispiel Geschäftsbereiche) umfassen kann (Dillon et al. 2010). Der Zugriff auf die Cloud wird unter der Verwendung eines Virtual Private Networks (VPN) realisiert. Die Cloud-Infrastruktur ist das Eigentum eines Cloud-Service-Providers. Sie wird durch den Cloud-Service-Provider betrieben und verwaltet, wobei der Cloud-Service-Kunde die vollständige Kontrolle über die virtuelle Netzwerkumgebung behält.

2.2 Fazit

Durch seine inhärenten Charakteristiken, seinen Service- und Bereitstellungsmodellen gilt Cloud Computing als zentraler Wachstumsmotor und Innovationstreiber mit dem Potenzial, die gesamte Informations- und Kommunikationstechnikbranche nachhaltig zu verändern. Das Cloud-Computing-Ökosystem ist jedoch durch Unsicherheiten und einem Mangel an Transparenz geprägt und die Adoption von Cloud-Services ist durch Hemmschwellen wie beispielsweise Sicherheitsrisiken, Kontrollverlust über die eigenen Daten und intransparenten Preismodellen geprägt (Lins et al. 2016b; Schneider and Sunyaev 2016; European Network and Security Agency 2012; Lang et al. 2016). Bei der Betrachtung der Risiken von Cloud Computing ergeben sich für jedes Service- und Bereitstellungsmodell individuelle Risiken (European Network and Security Agency 2012; Schneider and Sunyaev 2015). Zudem erfordern die einzigartigen Charakteristiken von Cloud Computing, wie beispielsweise die Vielzahl an Speicherlokationen und die Multi-Mandanten-Architektur, gesonderte Risikobewertungen und angepasste Bewältigungsstrategien (Heiser and Nicolett 2008). In diesem Zusammenhang können Zertifizierungen von Cloud-Services Entscheidungsträger bei der Auswahlentscheidung unterstützen, Transparenz am Markt schaffen, Vertrauen und Akzeptanz auf der Anwenderseite erhöhen sowie es Cloud-Service-Providern ermöglichen, ihre Systeme und Prozesse zu überprüfen und zu verbessern (Lins et al. 2016a; Lang et al. 2017).

2.3 Literaturverzeichnis

Amazon Web Services (2015) AWS | Amazon Virtual Private Cloud (VPC) – Sichere private Cloud (VPN). https://aws.amazon.com/de/vpc/. Accessed 22.06.2016.

Annette JR, Banu WA, Chandran PS (2015) Rendering-as-a-Service: Taxonomy and Comparison. Procedia Computer Science 50:276-281. doi:https://doi.org/10.1016/j.procs.2015.04.048.

Dašić P, Dašić J, Crvenković B (2016) Service Models for Cloud Computing: Search as a Service (SaaS). International Journal of Engineering and Technology 8 (5):2366-2373.

Dillon T, Wu C, Chang E (2010) Cloud Computing: Issues and Challenges. In: Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), Perth, Australia, 2010. pp 27-33.

European Network and Security Agency (2012) Cloud Computing - Benefits, Risks and Recommendations for Information Security. https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security. Accessed 22.06.2016.

Heiser J, Nicolett M (2008) Assessing the Security Risks of Cloud Computing. Gartner Inc. http://s3.amazonaws.com/academia.edu.documents/33355553/Gartner_Security_Risks_of_Cloud.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1498136359&Signature=GaUtYOBOYbyHlCcc3PFi1rqBMiA%3D&response-content-disposition=inline%3B%20filename%3DAssessing_the_Security_Risks_of_Cloud_Co.pdf. Accessed 22.06.2017.

Lang M, Wiesche M, Krcmar H (2016) What Are the Most Important Criteria for Cloud Service Provider Selection? A Delphi Study. In: Proceedings of the 24th European Conference on Information Systems (ECIS 2016), Istanbul, Turkey, 2016. pp 1-18.

Lang M, Wiesche M, Krcmar H (2017) Conceptualization of Relational Assurance Mechanisms - A Literature Review on Relational Assurance Mechanisms, Their Antecedents and Effects. In: Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, Switzerland, 2017. pp 852-866.

Leimeister S, Böhm M, Riedl C, Krcmar H (2010) The Business Perspective of Cloud Computing: Actors, Roles and Value Networks. In: Proceedings of the 18th European Conference on Information Systems (ECIS 2010), Pretoria, South Africa, 2010. pp 1-14.

Lins S, Grochol P, Schneider S, Sunyaev A (2016a) Dynamic Certification of Cloud Services: Trust, but Verify! IEEE Security and Privacy 14 (2):67–71.

Lins S, Schneider S, Sunyaev A (2016b) Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing. IEEE Transactions on Cloud Computing (forthcoming). doi:10.1109/tcc.2016.2522411.

Linthicum DS (2009) Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide: How to Use SaaS, SOA, Mashups, and Web 2.0 to Break Down the IT

Gates. 1 edn. Addison-Wesley, Boston, US.

Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2011) Cloud Computing — The Business Perspective. Decision Support Systems 51 (1):176–189.

Mell P, Grance T (2011) The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology, Gaithersburg; Montgomery; USA.

Schneider S, Sunyaev A (2015) Cloud-Service-Zertifizierung. Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services. 1 edn. Springer-Verlag, Berlin Heidelberg. doi:10.1007/978-3-662-47286-6.

Schneider S, Sunyaev A (2016) Determinant Factors of Cloud-sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing. Journal of Information Technology 31 (1):1-32. doi:10.1057/jit.2014.25.

Sharma DH, Dhote C, Potey MM (2016) Identity and Access Management as Security-as-a-Service from Clouds. Procedia Computer Science 79:170-174.

Soares J, Carapinha J, Melo M, Monteiro R, Sargento S (2011) Building Virtual Private Clouds with Network-aware Cloud. In: Proceedings of the 5th International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP 2011), Lisbon, Portugal 2011. pp 119-124.

Sunyaev A, Schneider S (2013) Cloud Services Certification. Communications of the ACM (CACM) 56 (2):33–36. doi:10.1145/2408776.2408789.

3 Kriterien für die Auswahl von Cloud-Services

M. Lang, C. Neubauer, A. Weiss, M. Wiesche, H. Krcmar

Cloud Computing spezifiziert ein neues Bereitstellungsmodell für IT-Services, welches die Art und Weise verändert, wie Unternehmen IT-Services konsumieren. Aufgrund des wachsenden Marktes für Cloud-Services untersucht dieses Kapitel die Herausforderungen, denen Organisationen beim Kauf von Cloud-Services gegenüberstehen. Auf der Grundlage aktueller Erkenntnisse in der organisatorischen Einkaufsliteratur, einer Delphi Studie zur Identifikation der wichtigsten Qualitätskriterien und bewährten Praktiken, zeigt dieses Kapitel die Herausforderungen und Lösungsansätze für die einzelnen Bestandteile eines Cloud-Service Einkaufsprozesses auf. Abgerundet wird das Kapitel durch eine Checkliste, welche für eine abschließende Überprüfung eines möglichen Cloud-Service-Providers herangezogen werden kann.

Cloud computing is a new deployment model for IT services, which is going to change the way organizations provision IT services substantially. As the market for cloud-services grows, this chapter investigates the challenges organizations face when purchasing cloud-services. Based on current findings in organizational purchasing literature, a Delphi study prioritising the most important quality criteria, and best practice, this chapter outlines a purchasing process and discusses challenges within each purchasing step. Finally, we provide a checklist, which can be adopted for a final verification test of possible cloud-service provider.

Das Forschungsprojekt NGCert wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) gefördert (Förderkennzeichen: 16KIS0078).

H. Krcmar et al. (Hrsg.), *Management sicherer Cloud-Services*,
https://doi.org/10.1007/978-3-658-19579-3_3

3.1 Entscheidungsfindung in der Cloud

Die Auslagerung vereinzelter oder gesamter IT-Prozesse in die Cloud ist ein komplexer Prozess mit drei aufeinander folgenden Schritten (Luoma and Nyberg 2011; Moe et al. 2017; Zhou et al. 2007). Zu diesen Schritten gehören die Entscheidung über die Auslagerung selbst, die Vorauswahl möglicher Cloud-Service-Provider und die finale Cloud-Service-Provider-Auswahl (Abbildung 3-1) (Moe et al. 2017).

Abbildung 3-1. Auslagerung von IT-Prozessen in die Cloud.

Im ersten Schritt treffen Cloud-Service-Kunden die Entscheidung über die Auslagerung der IT-Prozesse in die Cloud an sich. Besonders die Faktoren Gewohnheit und Erleichterung durch die Auslagerung in die Cloud beeinflussen die Entscheidungsfindung (Benlian and Hess 2011; Schneider and Sunyaev 2016). Während eine zunehmende strategische Bedeutung von Cloud-Services, verfügbaren Risiken oder wahrgenommener Komplexität Cloud-Service-Kunden davon abhalten, ihre Service-Prozesse in die Cloud auszulagern, sind es Faktoren wie Kosteneinsparungen, der Zugriff auf spezialisierte Ressourcen, erhöhte Flexibilität oder reduzierte Produkteinführungszeit, die den Cloud-Service-Kunden durch eine Auslagerung ermöglicht werden würden (Luoma and Nyberg 2011; Schneider and Sunyaev 2016). Beide Faktoren beeinflussen Cloud-Service-Kunden bei ihrer Entscheidungsfindung.

Im zweiten Schritt wählen Cloud-Service-Kunden mögliche Cloud-Service-Provider auf Basis funktionaler Anforderungen und Rahmenanforderungen für Daten aus. Es werden (meist) nur Cloud-Service-Provider beachtet, die das Bereitstellungsmodell (Infrastructure-as-a-Service, Platform-as-a-Service oder Software-as-a-Service) und benötigte Funktionen oder Anwendungen (bspw. CRM-Systeme) anbieten (Garg et al. 2013; Schrödl 2012). Rahmenanforderungen für Daten, z.B. sensible Daten, die spezifischen regulatorischen Anforderungen unterliegen, dienen als weitere Bewertungsgrundlage zur Bildung einer Liste vorausgewählter Cloud-Service-Provider (Rieger et al. 2013; Zhou et al. 2007). Die resultierende Liste der Cloud-Service-Provider bildet dabei die Entscheidungsgrundlage für eine spätere Auswahl des Cloud-Service-Providers (Garg et al. 2013; Schrödl 2012). Die Herausforderung besteht darin, den *"richtigen"* Cloud-Service-Provider zu finden, der von den Cloud-Service-Kunden benötigt wird, um im nächsten Schritt eine detaillierte Cloud-Service-Provider-Prüfung durchzuführen (Garrison et al. 2012; Garrison et al. 2015; Weinhardt et al. 2009).

Cloud-Service-Kunden müssen im dritten Schritt des Entscheidungsprozesses einen geeigneten Cloud-Service-Provider auswählen (Lang et al. 2017). Häufig erfüllen mehrere Cloud-

Service-Provider grundlegende Anforderungen an das erforderliche Service-Modell, erforderliche Funktionen oder Anwendungen (Garg et al. 2013). Zusätzlich zu den funktionalen Anforderungen und Rahmenanforderungen müssen Anforderungen an die Qualitätskriterien berücksichtigt werden (Garg et al. 2013). Zum Beispiel garantieren Cloud-Service-Provider unterschiedliche Verfügbarkeiten, die in der Regel zwischen 98% und 99,999% variieren. Cloud-Services haben eine hohe Diversität verschiedener Qualitätskriterien (Ghosh et al. 2015); Cloud-Service-Kunden müssen aus einer Fülle von Angeboten auswählen und entscheiden, welche Erfolgsfaktoren relevant sind und welche Cloud-Service-Provider ihre Anforderungen an Qualitätskriterien erfüllen können (Huang and Nicol 2013).

3.2 Ermittlung des Bedarfs an Cloud-Services

Nachdem der grundsätzliche Ablauf zum Einkauf von Cloud-Services spezifiziert wurde, wird in diesem Unterkapitel genauer erläutert, wie Cloud-Service-Kunden den Bedarf an Cloud-Services spezifizieren können.

Voraussetzung für die Spezifikation des Bedarfs an Cloud-Services ist eine Prozessanalyse, die im Unternehmen Anwendung finden. Hierbei können Engpässe und Optimierungspotenziale identifiziert und somit Startpunkte für die Bedarfsermittlung festgelegt werden. Empfehlenswert ist es an dieser Stelle, Angebote am Cloud-Markt zu observieren und mögliche Einsatzszenarien im Unternehmen zu spezifizieren. Als Illustrationsbeispiel sind grundlegende Prozessbestandteile von Unternehmen in Abbildung 3-2 dargestellt, sowie beispielhafte Cloud-Services den Prozessbestandteilen zugeordnet.

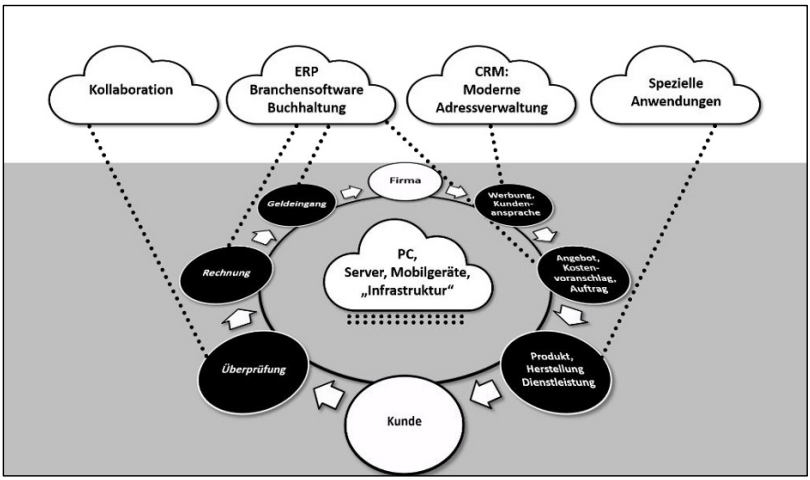

Abbildung 3-2. Unternehmensprozesse und typische Cloud-Services.

In Abbildung 3-2 stellen Unternehmen und Kunden die jeweiligen Eckpunkte dar, zwischen denen die Prozesse ablaufen. Um Umsätze zu generieren, ist es für Unternehmen von zentraler Bedeutung, Kunden anzuwerben. Hierbei sind persönliche Ansprachen der Kunden ein Erfolgskriterium, welches das Vorhandensein von Kundendaten bedingt. Angebote, Kostenvoranschläge und Aufträge müssen geschrieben werden und zur Weiterverarbeitung bereitstehen. Wird das Angebot angenommen, erfolgt die Bearbeitung. Je nach Unternehmen besteht die georderte Leistung aus einer Produktion, dem (Weiter-)Verkauf, dem Versand oder einer Dienstleistung. Nachdem der Kunde die Leistung erhalten und geprüft hat, erfolgt die Rechnungs- und Zahlungsbearbeitung. Damit schließt sich der Kreislauf zwischen Unternehmen und Kunden. Anhand dieser Prozessstruktur können verschiedene Einsatzgebiete für den Einsatz von Cloud-Services identifiziert werden.

Nachdem das Ergebnis einer Prozessanalyse die Einführung eines Cloud-Services empfiehlt, muss der genaue Bedarf spezifiziert werden. Hierbei können die folgenden Fragestellungen als Hilfestellung betrachtet werden:

- Welche Art von Cloud-Lösung suchen Sie?
- Wie sehen Ihre funktionalen und nicht funktionalen Anforderungen aus? (Siehe Kapitel 3.3)
- Bei welchen Prozessen bzw. für welche Aufgaben soll die Cloud-Lösung eingesetzt werden?
- Welche Funktionen sind Ihnen dabei besonders wichtig?
- Auf welche Funktionen können Sie notfalls verzichten?
- Wer soll in Ihrem Unternehmen mit der Lösung arbeiten?
- Welche Anforderung an Sicherheit und Datenschutz haben Sie?
- Gehören die zu verarbeitenden Daten unterschiedlichen Schutzklassen an?
- Gibt es unternehmensinterne oder rechtliche Restriktionen hinsichtlich der Datenverarbeitung (beispielsweise Compliance)?
- Was ist Ihnen hinsichtlich des Anbieters wichtig (z.B. Ortsnähe, persönlicher Kontakt)?
- Brauchen Sie Support vor Ort oder reicht Ihnen eine englischsprachige Telefonhotline?
- Wie schnell soll Ihnen der Support helfen können?
- Benötigen Sie Unterstützung bei der Implementierung des Service, z.B. in Form von einer Mitarbeiterschulung?
- Welche Anforderungen haben Sie an die Verfügbarkeit der Cloud-Lösung? Wie viel Stunden Ausfall sind für Sie maximal akzeptabel, wenn ein Rechenzentrum ausfallen sollte?
- Gibt es bestimmte Zeiten, zu denen der Cloud-Service einer besonderen Belastung ausgesetzt wird oder hoch verfügbar sein muss (z.B. hohe Systemauslastung im Saisongeschäft, Fristen gegenüber Behörden)?

3.3 Relevante Qualitätskriterien aus Kundensicht[3]

Nachdem der spezifische Bedarf identifiziert worden ist, gilt es einen geeigneten Cloud-Service auszuwählen. Aufgrund des kompetitiven Umfelds im Cloud-Markt sind die Preise allein kein Diversifizierungsmerkmal mehr. Daher müssen weitere Qualitätskriterien herangezogen werden. Im Folgenden wird daher aus Kundensicht eine Übersicht zu den wichtigsten Qualitätskriterien zur Auswahl eines Cloud-Services gegeben.

Tabelle 3-1 zeigt die der Kundenmeinungen nach wichtigsten 13 Qualitätskriterien bei der Auswahl von Cloud-Services und deren Erläuterungen auf. Die Ergebnisse wurden mittels Expertenbefragungen und einer anschließenden Priorisierung durch die Delphi-Methode erhoben. Details können der zugehörigen Veröffentlichung Lang et al. (2016) entnommen werden.

Tabelle 3-1. Relevante Qualitätskriterien aus Kundensicht (Quelle: Lang et al. (2016))

Qualitätskriterium		**Priorität**
Funktionalität	Die mit der Cloud-Lösung verbundenen Funktionen oder Fähigkeiten (Leistung, Verfügbarkeit, Sicherheit, Skalierbarkeit) entsprechend der Nachfrage des Cloud-Service-Kunden.	1
Gesetzes-konformität	Aufgrund der geografischen Lage, der Policen usw. entspricht ein Cloud-Service-Provider den gesetzlichen und aufsichtsrechtlichen Anforderungen des Cloud-Service-Kunden.	2
Vertragliche Gestaltung	Der Cloud-Service-Provider bietet verständliche vertragliche Vereinbarungen einschließlich einer klaren Kostenstruktur (z.B. Verbrauchsbezogenes Preismodell) an.	3
Geographischer Datenspeicherort	Die geographische Zuordnung der Datenspeicherung und ggf. auch Datenverarbeitung eignet sich in Bezug auf Datenschutzgesetzgebung und Benutzerlatenz.	4
Flexibilität	Ein Cloud-Service-Kunde kann die erhaltenen Fähigkeiten selbstständig anpassen und die Anpassungen werden innerhalb kurzer Zeit und mit transparenten Kosten automatisch durchgeführt.	5
Integration	Die Konfiguration des Cloud-Services ermöglicht eine reibungslose Integration in die IT-Landschaft des Unternehmens.	6
Transparenz der Aktivitäten rund um den Service	Transparenz von Sicherheit, Datenschutz, Datenzugriff, Cloud-Architektur, Service-Level-Kompetenzen usw.	7
Zertifizierung	Ein Cloud-Service-Provider wird von einer unabhängigen und vertrauenswürdigen Organisation gemäß den festgelegten Anforderungen oder Normen zertifiziert.	8
Überwachung	Eine manuelle oder automatisierte IT-Überwachung und Managementtechnik, die Transparenz der Cloud-Service-Qualität bietet.	9
Unterstützung	Ein Cloud-Service-Provider verfügt über eine reaktionsschnelle Serviceunterstützung, die alle operativen Prozesse für die Abwicklung von Serviceunterbrechungen und für die Implementierung von Änderungen bereitstellt.	10
Kontrolle	Ein Cloud-Service-Provider bietet Fernzugriffstools, um eine proaktive Steuerung von Daten, Funktionalitäten und Prozessen (z.B. Anpassung) zu ermöglichen.	11
Betriebsmodell	Ein klar definiertes Bereitstellungsmodell in Bezug auf Besitz, Kontrolle der architektonischen Gestaltung und Grad der verfügbaren Anpassung (z.B. Private Cloud, Hybrid Cloud, Community Cloud, Public Cloud).	12
Test der Lösung	Ein Cloud-Service-Provider ermöglicht bequeme Testzeiten eines Cloud-Services.	13

[3] Aufbauend auf der bereits von Lang et al. (2016) durchgeführten Studie zum Thema dieses Abschnitts werden nachfolgend die wesentlichen Aspekte kurz zusammengefasst.

Um besser zu verstehen, was die wichtigsten Qualitätskriterien sind, wurden die drei durchgeführten Entscheidungsrunden der durchgeführten Delphi-Methode miteinander verglichen. Interessanterweise blieb die Rangfolge der fünf wichtigsten Qualitätskriterien (Funktionalität, Gesetzeskonformität, vertragliche Gestaltung, geographischer Datenspeicherort, Flexibilität) während jeder Iteration stabil. Dieses Ergebnis deutet auf einen hohen und stabilen Konsens unter den Entscheidungsträgern hin, wodurch die Top-5 Qualitätskriterien als ein universeller Indikator für die wichtigsten Qualitätskriterien während der Auswahlentscheidung der Cloud-Service-Provider interpretiert werden können.

Im Gegensatz dazu änderte sich die Priorität der Qualitätskriterien in den Rangfolgen von 6 bis 13 in den Iterationen leicht. Dies deutet darauf hin, dass die Qualitätskriterien der Cloud-Service-Provider zwischen Rang 6 bis 13 individuell variieren können und dementsprechend angepasst werden müssen.

3.4 Checkliste zur Auswahl des ‚richtigen' Cloud-Services

Ist ein geeigneter Cloud-Service-Provider identifiziert worden, sollte eine abschließende Detailprüfung stattfinden. Diese Detailprüfung soll sicherstellen, dass die geforderten Mindestanforderungen erfüllt werden, Datenschutz- und Datensicherheitsaspekte eingehalten werden, sowie der langfristige Betrieb gewährleistet ist.

Tabelle 3-2 gibt die wichtigsten Aspekte wieder, die zu den Dimensionen Anbieter, Vertrag, Datenschutz und Datensicherheit, Rechenzentrum, Betriebsprozesse und Service aus Kundensicht überprüft werden sollten. Für eine vollständige Übersicht aller Aspekte wird auf TrustedCloud (2016) verwiesen[4].

Tabelle 3-2. Checkliste zur Auswahl eines Cloud-Services

Checkliste zur Adaption von Cloud-Services		Hintergrund
Anbieter		
1	Gibt es eine genaue Servicebeschreibung?	Zur Klärung der funktionalen Anforderungen in Bezug auf den Unternehmensbedarf und der zugesicherten Leistungen.
2	Wer ist der rechtliche Vertragsgeber und sind Beteiligungsverhältnisse geklärt?	Zur Prüfung des möglichen Einflusses durch beherrschende Gesellschafter.
3	Sind Besitzer und Standorte der Rechenzentren offengelegt?	Zur Klärung der Datenstandorte und beteiligter Subunternehmer zur Erfüllung der Kontrollfähigkeit.
Vertrag und Vertragsbestandteile		
4	Ist das anwendbare Recht im Vertrag ausgewiesen?	Zumindest der Rechtsstandort bei möglichen Auseinandersetzungen sollte angegeben sein.

[4] Eine noch weitergehende Vertiefung finden Sie zum Beispiel im Zertifizierungsschema Star Audit: https://staraudit.org/de.html